(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2001 (04.01.2001)

PCT

(10) International Publication Number
WO 01/01629 A1

(51) International Patent Classification⁷: H04L 9/32, 9/30

(21) International Application Number: PCT/EP00/05642

(22) International Filing Date: 19 June 2000 (19.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1012435 25 June 1999 (25.06.1999) NL

(71) Applicant *(for all designated States except US)*: KONINKLIJKE KPN N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DE BOER, Marten [NL/NL]; Egypte 2, NL-9285 WX Buitenpost (NL). KLEINHUIS, Geert [NL/NL]; Mindertfaen 1, NL-9264 TX Eernwoude (NL).

(74) Agent: KLEIN, Bart; Koninklijke KPN N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

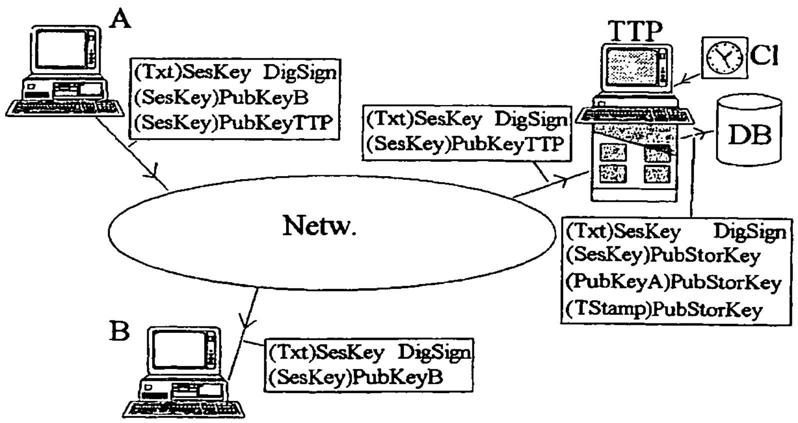
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR PROTECTED STORAGE AND MANAGEMENT IN A TTP SERVER



(57) Abstract: System for protected storage in a TTP server. A file (Txt) is transmitted from a first (A) to a second user (B) after being enciphered with a session key (SesKey), which is enciphered with the public key (PublKeyB) of the second user. The session key (SesKey) is also enciphered by the first user with the public key (PublKey/TTP) of the TTP server which, after having received it, deciphers said session key with his private key (SecKeyTTP). The TTP server subsequently enciphers the session key (SesKey) and the (original) public key (PubKeyA) of the first user (A) with a "public" storage key (PubStorKey). The enciphered session key ((SesKey)PubStorKey) and public key ((PubKeyA)PubStorKey) of the first user are stored, together with the enciphered file ((Txt)SesKey), in a storage medium (DB). They are recoverable by the TTP, by deciphering with the private storage key (SecStorKey), and may be transmitted after having been enciphered with the current public keys (PubKeyA' or PubKeyB', as the case may be) of the users.

WO 01/01629 A1

System for protected storage and management in a TTP server.

BACKGROUND OF THE INVENTION

The invention relates to a system for protected storage and management in a TTP server [TTP = Trusted Third Party] of copies of digital files transmitted, by way of a transmission channel, from a first to a second user.

The invention relates to, in other words, a timeless key and storage system for the benefit of the long-term storage of electronically exchanged (digitally protected) information and protectedly making available (secure retrieving) the stored data.

The few known systems have the following drawbacks:

1) Current protection techniques have a restricted hackability duration guarantee.
2) Limited protection guarantees prior to, during and after long-term storage.
3) Much storage space and effort are required for key management.
4) Protected long-term storage and the associated key and storage management is now either not regulated or very complex in setup.
5) Due to the ever changing software and hardware, it is very difficult to guarantee electronic timelessness.

B. SUMMARY OF THE INVENTION

The object of the invention is to overcome said drawbacks. For this purpose, the invention provides for a system having means for carrying out the functionalities: "Secure Archiving", "Re-encryption" and "Secure Retrieval", which will be discussed below. In this connection, the optional items "Digital Sign" and "Time Stamp" will be discussed separately.

"Secure Archiving"

If, according to the current state of the art, a file is transmitted from a first user to a second user in a safe way, the file is enciphered with a symmetrical session key, which in its turn is enciphered with the public key of the second user. Said second user may decipher the session key with his private key and decipher the file itself with the session key deciphered in this manner.

According to the invention, the session key is also enciphered by the first user with the public key of an "in-line" TTP server (i.e., included in the transmission channel between the first and second users), which TTP server deciphers the session key received with his private key. Thereafter, the TTP server enciphers the deciphered session key with a "public" storage key. The session key enciphered with said public storage key and the file enciphered with the session key are subsequently stored in a storage medium of the TTP.

It should be noted that above and below there is spoken of public and private keys. These are generally known. In general, a public and a private key constitute an asymmetric pair of keys. If a file or a code is enciphered with the public key of an asymmetric pair of keys, said file or code may be deciphered only with the help of the associated private key and vice versa. In general, the public keys are available to "the public", e.g., by way of a publicly accessible data base, such as www.pgp.com. In the present application, it is assumed that the users and the TTP each dispose of a pair of keys, each consisting of a public and a private key, and in particular intented for protecting the mutual data exchange of the files and codes. In addition, the TTP disposes of a pair of keys which is used within the TTP only; the "public" and private keys serve as protected storage or recovery ("secure retrieval"), as the case may be, of files and codes. The public storage key is not, as is normally the case for public keys, put at the disposal of the public.

"Re-encryption"

By way of "periodic maintenance" - from security considerations - the TTP server may at regular points in time store the file once again in the storage medium. For this purpose, the session key with which the file was enciphered is first recovered by deciphering - with the private storage key - the stored (enciphered) session key. Subsequently, the enciphered file stored in the storage medium is deciphered with the recovered session key.

The TTP server then generates a new asymmetric pair of storage keys, consisting of a new public storage key (which is not made available outside the TTP) and a new private storage key, and a new version of the symmetrical session key, whereafter the TTP enciphers the deciphered file with the new session key and stores it in the storage medium.

The TTP also enciphers the new session key with the new public storage key and stores said enciphered session key in the storage medium.

"Secure Retrieval"

For protected recovery of the stored file, and transmission thereof to the first and/or second user, the symmetrical session key is recovered from the storage medium by deciphering, with the private storage key, the stored enciphered session key. The recovered session key is subsequently enciphered with the current public key of the first or second user, as the case may be, and transmitted to said user by way of the transmission channel, together with a copy of the file stored in the storage medium, enciphered with the session key. After having received the enciphered session key, the user may recover the session key therefrom by deciphering with his private key. Subsequently, the user may decipher the file enciphered with the session key using the recovered session key.

"Digital Sign"

The public key of the first user may - as is well-known - be used to verify a digital signature of the file. A problem arises if - which frequently occurs - the first user at a certain point in time, after the file has been stored in the TTP server, generates a new pair of keys (comprising a public and a private key) and discontinues the old one. For this reason, it is of importance to store the (original) public key of the first user in the TTP server, since only said original key may be used for verifying the digital signature of the stored, later retrievable file.

For this case, the TTP server, after having received the enciphered file, also enciphers the - at that point in time publicly available - public key of the first user, with the public storage key, and stores said enciphered public key in the storage medium.

Periodically, the TTP server — as "periodical maintenance" — deciphers the enciphered (original) public key, stored in the storage medium, of the first user having the private storage key, and enciphers the deciphered public key of the first user having the newly generated public storage key, and stores said freshly enciphered key in the storage medium.

The public key of the first user may — upon retrieving the stored file — be recovered from the storage medium by deciphering, with the private storage key, said stored key. The public key of the first user recovered in this manner is subsequently enciphered with the — at that point in time publicly available -- public key of the retrieving first or second user, and transmitted by way of the transmission channel. After having received said enciphered public key, the user may recover the original public key of the first user by deciphering his current private key; subsequently, the digital signature of the recovered file may be verified using the recovered original public key of the first user.

"Time Stamp"

If so desired, the TTP server, after the enciphered file has been received and stored, may generate a time stamp and store it, linked to the stored file and enciphered with the public storage key, in the storage medium. In the event of retrieving the stored file by the first or second user, the time stamp is deciphered and subsequently enciphered with the public key valid for said user and transmitted to the user. The user may decipher the enciphered time stamp with his current private key.

DESCRIPTION OF THE FIGURES

Below, the invention is illustrated in further detail by reference to several figures. Figures 1, 2 and 3 illustrate the functions "Secure Archiving", "Re-encryption" and "Secure Retrieval", including the items "Digital Sign" and the "Time Stamp".

FIG. 1: "Secure Archiving"

A file **Txt** is transmitted from a first user **A** to a second user **B** after having been enciphered with a symmetical session key **SesKey**. Said session key is enciphered with the public key **PubKeyB** of the second user. The latter may decipher the session key with his private key **SecKeyB** and the file itself with the deciphered session key.

The session key is also enciphered by the first user with the public key of the TTP server **PubKeyTTP**, which, after having received it, deciphers said session key with his private key **SecKeyTTP**. Thereafter the TTP server enciphers the deciphered session key with a "public" storage key **PubStorKey** of the TTP.

The (transmission) keys of the users A and B each form an asymmetrical pair of keys, **KeyPairA** and **KeyPairB**, respectively, consisting of **PubKeyA** and **SecKeyA**, and **PubKeyB** and **SecKeyB**, respectively. The TTP uses the pair of keys **KeyPairTTP**, consisting of **PubKeyTTP** and **SecKeyTTP**. Finally, for the protected storage of an asymmetrical pair of keys **StorKeyPair**, consisting of the keys **PubStorKey** and **SecStorKey**; contrary to the preceding public keys, **PubStorKey** nor **SecStorKey** is publicly available, but is used exclusively within the TTP.

The session key **(SesKey)PubStorKey** enciphered with the public storage key **PubStorKey** and the file **(Txt)SesKey** enciphered with the session key **SesKey** are subsequently stored in the storage medium **DB** of the TTP.

"Digital Sign"

The public key **PubKeyA** of the first user **A** may be used to verify a digital signature **DigSign** of the file **Txt**. In this case, the TTP server, after having received the enciphered file **(Txt)SesKey**, also enciphers the - at that point in time publicly available - public key **PubKeyA** from the first user **A**, with the public storage key **PubStorKey**, and stores said enciphered public key **(PubKeyA)PubStorKey** in the storage medium **DB**.

"Time Stamp"

After having received and stored the enciphered file **(Txt)SesKey**, the TTP server may generate a time stamp **TStamp** and store it, after enciphering with the public storage key **PubStorKey** and linked to the stored file, in the storage medium **DB** as **(TStamp)PubStorKey**.

FIG. 2: "Re-encryption"

As "periodical maintenance", the TTP server deciphers the enciphered file **(Txt)SesKey** stored in the storage medium with the session key **SesKey**, which for that purpose is recovered by deciphering the stored session key **(SesKey)PubStorKey** with the private storage key **SecStorKey**. The TTP server subsequently generates a fresh pair of storage keys **StorKeyPair**, comprising a new "public" storage key **PubStorKey'** and a new private storage key **SecStorKey'**, as well as a new version of the symmetrical session key **SesKey'**. The TTP subsequently enciphers the deciphered file **Txt** with the new session key **SesKey'** and stores the file **(Txt)SesKey'** enciphered in this manner in the storage medium **DB**.

The TTP also enciphers the new session key with the new public storage key **PubStorKey'** and stores the session key **(SesKey')PubStorKey'** enciphered in this manner in the storage medium **DB**.

"Digital Sign"

During the periodical maintenance, the TTP server also deciphers the enciphered public key **(PubKeyA)PubStorKey** stored in the storage medium of the first user with the private storage key **SecStorKey**, and subsequently enciphers the deciphered public key **PubKeyA** with the newly generated public storage key **PubStorKey'** and stores the public key **(PubKeyA)PubStorKey'** enciphered in this manner in the storage medium.

"Time Stamp"

During the periodical maintenance, the TTP server also deciphers the enciphered time stamp **(TStamp)PubStorKey** stored in the storage medium with the private storage key **SecStorKey**, and subsequently enciphers the deciphered time stamp with the newly generated public storage key **PubStorKey'** and stores the time stamp **(TStamp)PubStorKey'** enciphered in this manner in the storage medium.

FIG. 3: "Secure Retrieval"

For protected recovery of the file **Txt**, and the transmission thereof to the first and second users **A** and **B**, respectively, the symmetrical session key **SesKey** is recovered from the storage medium by deciphering, with the private storage key **SecStorKey**, the stored enciphered session key **(SesKey)PubStorKey**. The recovered session key **SesKey** is subsequently enciphered with the then current public key **PubKeyA`** or **PubKeyB`**, as the case may be, from the querying first or second user **A** or **B**, as the case may be, and transmitted to said user by way of the transmission channel, together with a copy of the file stored in the storage medium, with the user, after having received the enciphered session key **(SesKey)PubKeyA˜** or **(SesKey)PubKeyB˜**, being capable of recovering the session key therefrom by deciphering, with his private key **SecKeyA˜** or **SecKeyB˜**, as the case may be, and subsequently being capable of deciphering the file **(Txt)SesKey** using the recovered session key.

"Digital Sign"

The original public key **PubKeyA** of the first user, necessary for verifying the digital signature of the recovered file, may be recovered from the storage medium by deciphering, with the private storage key **SecStorKey**, the stored public key **(PubKeyA)PubStorKey** of the first user enciphered with the public storage key. The deciphered public key **PubKeyA** of the first user recovered in this manner is subsequently enciphered with the current public key **PubKeyA˜** or **PubKeyB˜**, as the case may be, of the retrieving first or second user **A** or **B**, as the case may be, and transmitted to the user by way of the transmission channel. After having received said enciphered public key **(PubKeyA)PubKeyA˜** or **(PubKeyA)PubKeyB˜**, as the case may be, the user may recover the original public key **PubKeyA** of the first user therefrom by deciphering, with his current private key **SecKeyA˜** or **SecKeyB˜**, as the case may be. Subsequently, the digital signature **DigSign** of the file **Txt** may be verified using the recovered public key **PubKeyA** of the first user.

It should be noted that it is preferable to - otherwise than is shown in FIG. 3 - not transmit the digital signature **DigSign** uncipheredly to the first or second user, as the case may be, but enciphered with the public key of user **A** or **B**, as the case may be: instead of **"DigSign"**, the TTP server then transmits **"(DigSign)PubKeyA˜"** or **"(DigSign)PubKeyB˜"**, as the case may be. At the user's side, the digital signature may be recovered by deciphering, with the private keys of **A** and **B**, **SecKeyA** and **SecKeyB**, respectively.

"Time Stamp"

When the stored file is retrieved by the first or second user, the time stamp is first retrieved by deciphering

(TStamp)PubStorKey with the private storage key **SecStorKey**. The recovered time stamp is subsequently enciphered with the user's current public key **PubKeyA'** or **PubKeyB'**, as the case may be, and transmitted to said user. Thereafter, the user may decipher the enciphered time stamp **(TStamp)PubKeyA'** or **(TStamp)PubKeyB'**, as the case may be, with his current private key **SecKeyA'** or **SecKeyB'**, as the case may be.

CLAIMS

1. System for protectedly storing and managing, in a TTP server, copies of digital files which are transmitted, by way of a transmission channel, from a first to a second user, characterised in that

- a file (Txt) is transmitted from the first user (A) to a second user (B) after having been enciphered with a symmetrical session key (SesKey), which session key is enciphered using the public key (PubKeyB) of a first asymmetrical pair of keys (KeyPairB) associated with the second user, which second user, after having received it, may decipher the session key using the private key (SecKeyB) of said first asymmetrical pair of keys (KeyPairB) and subsequently may decipher the file using the session key deciphered in this manner, the session key (SesKey) also being enciphered by the first user (A) using the public key (PubKeyTTP) of a second asymmetrical pair of keys (KeyPairTTP) associated with the TTP server, which TTP server, after having received it, deciphers said session key using the private key (SecKeyTTP) from said second asymmetrical pair of keys (KeyPairTTP), whereafter the TTP server enciphers the deciphered session key (SesKey) using the public key of a third asymmetrical pair of keys (StorKeyPair), hereinafter to be referred to as public storage key (PubStorKey), and stores the session key ((SesKey)PubStorKey) enciphered with said storage key, together with the file ((Txt)SesKey) enciphered with the session key (SesKey), in a storage medium (DB).

2. System according to claim 1, characterised in that, periodically,

- the TTP server deciphers the enciphered file ((Txt)SesKey) stored in the storage medium with the session key (SesKey), which for that purpose is recovered in advance by deciphering the stored enciphered session key ((SesKey)PubStorKey) with the private key of the third pair of keys (StorKeyPair), hereinafter to be referred to as the private storage key (SecStorKey);

- the TTP server subsequently generates a new version of the third pair of keys, comprising a new public storage key (PubStorKey') and a new private storage key (SecStorKey'), and a new version of the symmetrical session key (SesKey'), whereafter the TTP enciphers the deciphered file (Txt) with the new session key (SesKey') and stores the file ((Txt)SesKey') enciphered in this manner in the storage medium (DB);
- the TTP server enciphers the new session key (SesKey') with the new public storage key (PubStorKey') and stores the session key ((SesKey')PubStorKey') enciphered in this manner in the storage medium (DB).

3. System according to claim 1, characterised in that, for protected recovery of the file (Txt) and transmission thereof to the first user (A) or the second user (B), as the case may be, the symmetrical session key (SesKey) is recovered from the storage medium by deciphering, with the private storage key (SecStorKey), the stored enciphered session key ((SesKey)PubStorKey), whereafter the recovered session key (SesKey) is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted to the user by way of the transmission channel, together with a copy of the file ((Txt)SesKey) stored in the storage medium, with the user, after having received the enciphered session key ((SesKey)PubKeyA' or (SesKey)PubKeyB', as the case may be), being capable of recovering the session key therefrom by deciphering using the user's private key (SecKeyA' or SecKeyB', as the case may be), and subsequently being capable of deciphering the enciphered file ((Txt)SesKey) using the recovered session key.

4. System according to claim 1, the public key (PubKeyA) of the first user (A) being used to verify a digital signature (DigSign) of the file (Txt), characterised in that the TTP server, after having received the enciphered file ((Txt)SesKey), also enciphers the then current public key (PubKeyA) of the first user (A) using the public storage key (PubStorKey), and stores said enciphered public key ((PubKeyA)PubStorKey) in the storage medium (DB).

5. System according to claim 4, characterised in that, periodically,

- the TTP server deciphers the enciphered public key (PubKeyA) of the first user stored in the storage medium with the private storage key (SecStorKey);
- the TTP server subsequently generates a new version of the third pair of keys, comprising a new public storage key (PubStorKey') and a new private storage key (SecStorKey');
- the TTP server enciphers the deciphered public key (PubKeyA) of the first user with the new public storage key (PubStorKey') and stores said public key ((PubKeyA)PubStorKey'), enciphered in this manner, in the storage medium.

6. System according to claim 4, characterised in that the public key (PubKeyA) of the first user is recovered from the storage medium by deciphering, with the private storage key (SecStorKey), the stored enciphered public key ((PubKeyA)PubStorKey) of the first user,
that said original public key (PubKeyA) recovered in this manner is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted by way of the transmission channel to the first or second user, as the case may be, with the user, after having received said enciphered public key ((PubKeyA)PubKeyA' or (PubKeyA)PubKeyB', as the case may be) being capable of recovering the original public key (PubKeyA) of the first user therefrom by deciphering with his current private key (SecKeyA' or SecKeyB', as the case may be), and subsequently being capable of verifying the digital signature (DigSign) of the file (Txt) using the original public key (PubKeyA) of the first user recovered in this manner.

7. System according to claim 6, characterised in that the digital signature (DigSign) is enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted to said first or second user, as the case may be, whereafter the receiving user recovers the digital signature by deciphering the

received, enciphered digital signature ((DigSign)PubKeyA' or (DigSign)PubKeyB', as the case may be) with his private key (SecKeyA' or SecKeyB', as the case may be).

8. System according to claim 1, characterised in that the TTP server, after having received the enciphered file ((Txt)SesKey) generates a time stamp (TStamp) and stores it, linked to the stored file and enciphered with the public storage key (PubStorKey), in the storage medium (DB).

9. System according to claim 8, characterised in that, in the event of retrieving the stored file by the first or second user (A or B, as the case may be) the enciphered time stamp ((TStamp)PubStorKey) is recovered by deciphering with the private storage key (SecStorKey), the recovered time stamp is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) for the querying user, and is transmitted to said user, whereafter the user may decipher the enciphered time stamp ((TStamp)PubKeyA' or (TStamp)PubKeyB', as the case may be) with the private key (SecKeyA' or SecKeyB', as the case may be) current for said user.

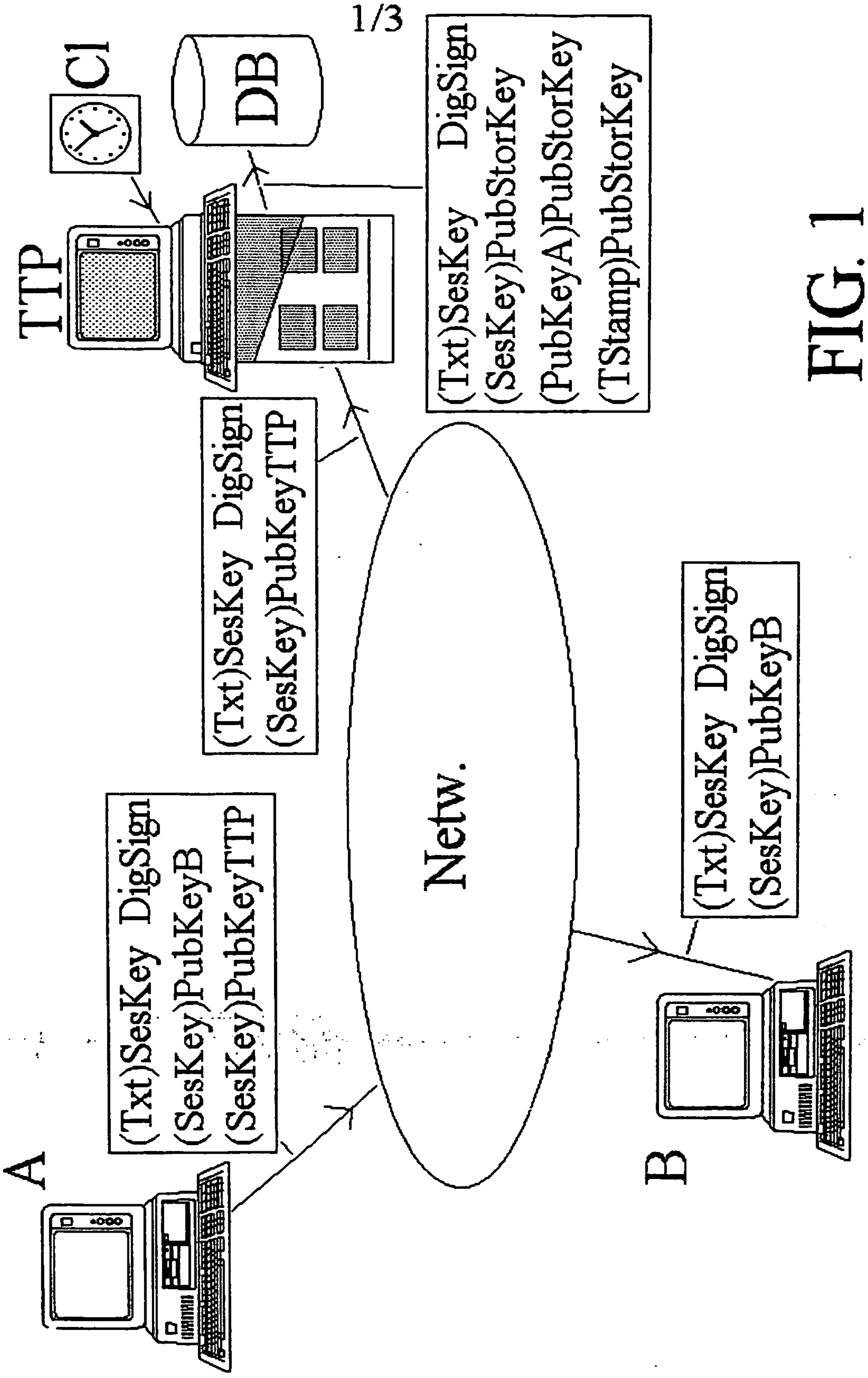

TTP
Cl
DB
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
(Txt)SesKey DigSign
(SesKey)PubKeyTTP
Netw.
A
(Txt)SesKey DigSign
(SesKey)PubKeyB
(SesKey)PubKeyTTP
B
(Txt)SesKey DigSign
(SesKey)PubKeyB

FIG. 1

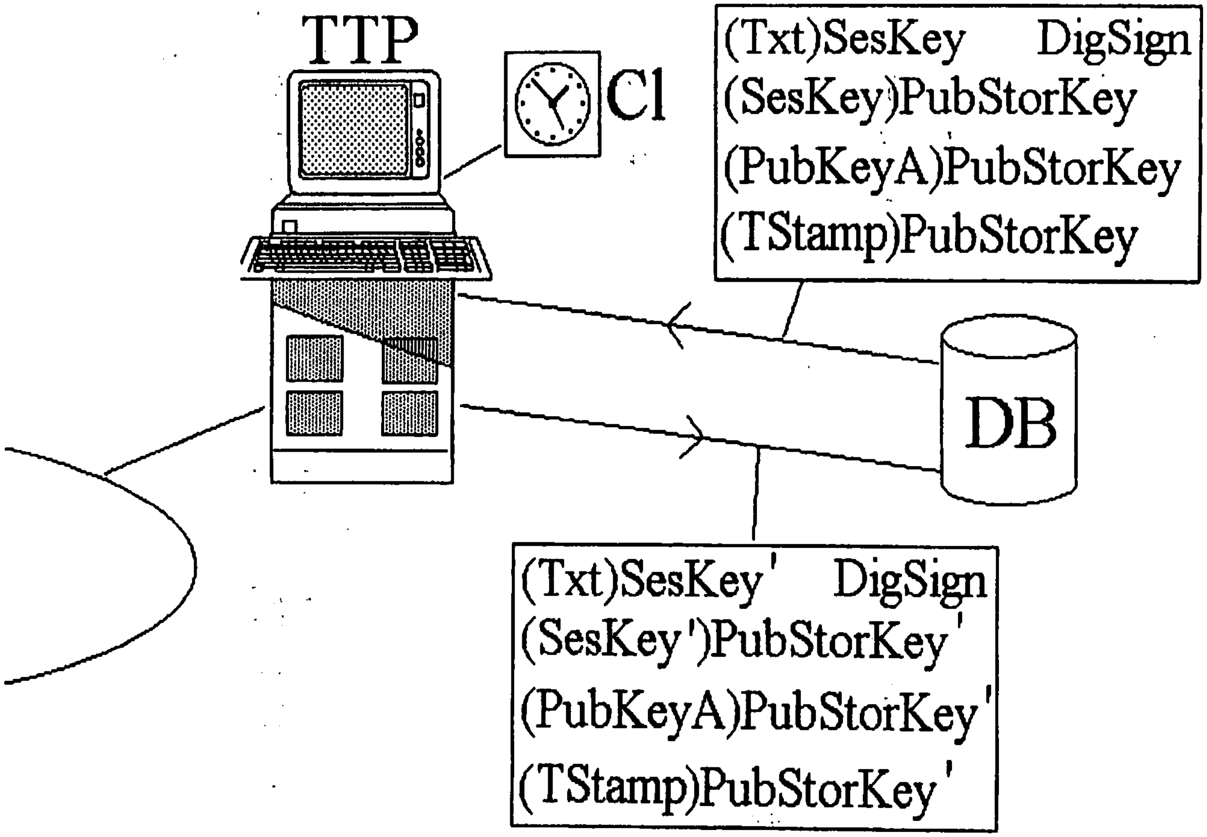

TTP
Cl
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
DB
(Txt)SesKey' DigSign
(SesKey')PubStorKey'
(PubKeyA)PubStorKey'
(TStamp)PubStorKey'

FIG. 2

3/3

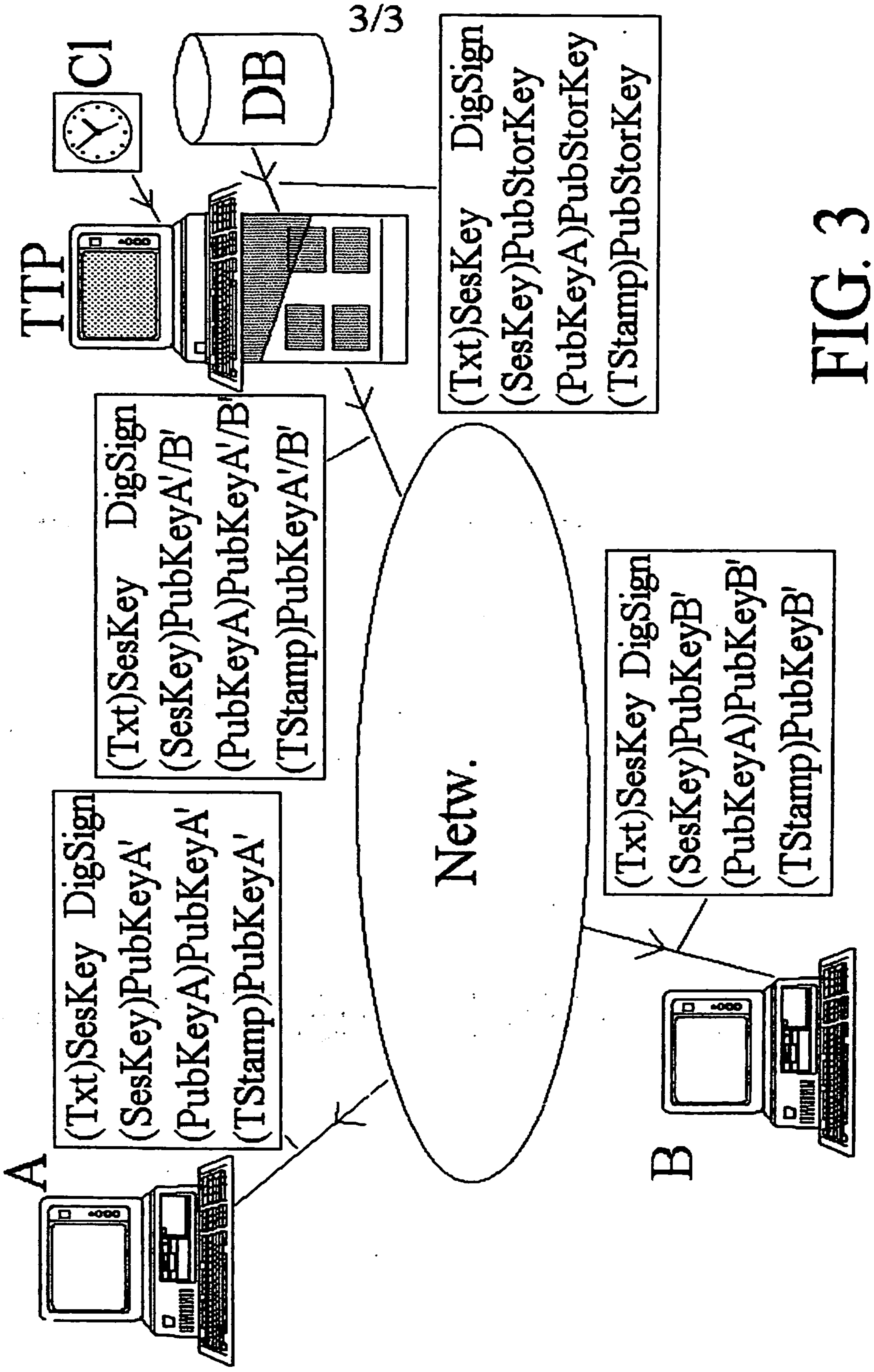

TTP
Cl
DB
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
(Txt)SesKey DigSign
(SesKey)PubKeyA'/B'
(PubKeyA)PubKeyA'/B'
(TStamp)PubKeyA'/B'
Netw.
(Txt)SesKey DigSign
(SesKey)PubKeyA'
(PubKeyA)PubKeyA'
(TStamp)PubKeyA'
A
(Txt)SesKey DigSign
(SesKey)PubKeyB'
(PubKeyA)PubKeyB'
(TStamp)PubKeyB'
B

FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 00/05642

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 892 521 A (HEWLETT PACKARD CO) 20 January 1999 (1999-01-20) figures 3,5C column 13, line 17 - line 24 column 14, line 8 - line 12 column 20, line 34 - line 45	1-9
A	DENNING D E ET AL: "A taxonomy for key escrow encryption systems" COMMUNICATIONS OF THE ACM, MARCH 1996, ACM, USA, vol. 39, no. 3, pages 34-40, XP000676295 ISSN: 0001-0782 page 39 -page 40; table 1	1-9
A	EP 0 422 757 A (FISCHER ADDISON M) 17 April 1991 (1991-04-17) column 3, line 58 -column 12, line 14	8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 10 August 2000	Date of mailing of the international search report 18/08/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Zucka, G

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 00/05642

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0892521 A	20-01-1999	JP 11119650 A	30-04-1999
EP 0422757 A	17-04-1991	US 5001752 A	19-03-1991
		AT 144360 T	15-11-1996
		AU 624299 B	04-06-1992
		AU 5753190 A	18-04-1991
		CA 2018770 A	13-04-1991
		DE 69028894 D	21-11-1996
		DE 69028894 T	03-04-1997
		JP 3185551 A	13-08-1991
		US 5136643 A	04-08-1992